Proceedings International Conference of Technology Management, Business and Entrepreneurship 2012 (ICTMBE2012),
Renaissance Hotel, Melaka, Malaysia 18-19 Dec 2012

A CRITICAL EXAMINATION OF ONLINE BANKING SCAM IN NIGERIA: KANO METROPOLIS IN VIEW

Alhaji Abubakar Aliyu[1], Rosmaini Bin Tasmin[2] and Josu Takala[3]

[12]Department of Technology Management,
Faculty of Technology Management and Business,
University Tun Hussein Onn Malaysia, 86400, Parit Raja, Batu Pahat, Darul Ta'zim, Johor, Malaysia
gp110047@siswa.uthm.edu.my

[3]Department of Production, University of Vaa'sa, City of Vaa'sa, Finland

ABSTRACT

Electronic banking frauds are becoming a global phenomenon in nature, while its consequences are becoming a great concern for the banks worldwide. This paper tries to investigate the magnitude of online banking frauds in Nigerian commercial banks and proffer lasting solutions that will mitigate this contending and boiling issue in the Nigerian banking industry. The paper employs both primary and secondary data in order to investigate the online banking frauds in Nigerian banks. The chi-square statistical technique was used to analyze the data and test the hypothesis raised. The paper concludes that both bank customers and bankers have a joint role to play in stopping the perpetrators of online banking frauds in the banks. The research reveals that phishing attacks appear to be the dominant dimension of online banking frauds in Nigeria followed by fake web site substitution and pharming. While, vishing fraud is not a common phenomenon in Nigeria, it ranked lowest in the ranking of the dimensions.

KEYWORDS: Online Banking Fraud, Malicious Code, Phishing attacks, Malware, Pharming

1. INTRODUCTION

Electronic banking has in particular brought about a paradigm shift in the banking services in Nigeria. Online banking, which is a branch of electronic banking service, is intended mainly to achieve two objectives. First, is to increase the convenience of banking transaction to the consumer; secondly is to reduce the cost of operations to the banks (Auta, 2010; Singhal and Padhmanabhan, 2008; Musa and Hassan, 2009; Agbolade, 2011 and Howard *et al.*, 2008). The ease of settlement of bills such as electricity, school fees, phone bills, insurance premium, travelling bills, transfer money between accounts and scheduling automatic periodic payments such as rent or loan payments, applying for accounts or loans, online viewing of account details and statement information; all this contributed immensely the use of online banking (Metropolis, 2010). In the process, banks are able to reduce cost of operations to some extent (Olatokun and Science, 2009). Although, online banking continues to present challenges to financial security and personal privacy but still millions of people have had their checking accounts compromised, mainly as a result of online banking fraud. Its

apparently clear that online banking crimes had undermined its success as few bank customers prepare the boring bank queues for secure transactions (Safeena and Kammani, 2011; Safeena and Lake 2010; Needs et al., 2007; Attacks, 2007; Singh, 2007; Alexander, 2004a and Musa and Hassan, 2009).

The convenience and safety in the use of online banking have been instrumental in increasing both volumes and used in the banking industry (Aliyu and Tasmin, 2012a; Aliyu and Tasmin, 2012b; Adeoti, 2011; Shittu, et al., 2010; Olatokun, 2009; Bankole and Brown 2011; Anyasi and Otubu, 2009; Sangeetha and Mahalingam, 2011 and Penang and Kheng, 2010a, 2010b). The growth of electronic banking services in Nigerian banks rose from 73% in 2009, 85% in 2010 to 289% in 2011. Today, all the banks in Nigeria introduced the use of online banking at their web site in 2012. The increase in the number of customers using online banking has also increased the propensity to fraudulent practices by the online banking fraud perpetrators. Today, commercial banks have gone into a massive awareness campaign through posters; jingles, pliers, radio and TV advert on the benefit of online banking and how customers should take the edge off the online banking frauds. Apparently, banks with large number of customer base like First bank, GT Bank, Zenith Bank, UBA and FSMB are continue leading the pack in number of transactions carried out through Electronic banking services in Nigeria. However, the number of transactions of online banking in the banking industry remains a significant measure of the efficiency of these online banking. Such transaction volumes can also be used to measure the kind of returns banks are getting from the regular patronage of their online banking. (Adeoti, 2011; John and Kaka, 2011; Akinlolu and Oyesola, 2008 and Dutta and Mia, 2010).

2. LITERATURE REVIEW

Online Banking fraud is defined as the act of stealing money from unsuspecting users via the Internet. Those, banks are so, worry about how their customers, and potential customers, perceive their services via the internet. The fear that always strikes the banking industry is if customers choose a particular bank over another base on the bank pass track record on security, or lack thereof, it could impact securing a new banking customer. Bank customers must feel their assets are safe, and for banks to remains relevant and scale throw in the near future, they must demonstrate this to the banking community. Research has proven that those are the high expectations of customers to their Banks.

Therefore, to fortress the point above, Adeloye (2008) identified security issues related to online banking as well as power outage as the primary challenges facing the electronic banking services in Nigeria. Whereas Voice and President (2005) and Singh (2007) identified various forms of online banking frauds, which include the following: -

2.1 Phishing Attacks

Phishing, the act of stealing customer's information via the internet for the purpose of committing online banking fraud, has become a significant criminal activity on the Electronic banking services. Phishing basically involves the use of fake email messages from the Bank or different individual pretending to be a Bank representative. Mostly, the email seeks customer to make available sensitive information such as name, password, account number etc. and provides links to a counterfeit web site, in which the tricks are the ones a customer follow the link and provide the requested information, intruders can have access to his/her personal account information and finances. While,

in some cases popup windows can appear in front of a copy of a genuine bank web site. The real web site address is displayed; however, any information a customer typed directly into the popup will go to unauthorized users. Conversely, as banks are consistently coming up with different strategies to defeat fraudsters, so also the fraudsters are in constant developing their means to defraud customers. Today, Hi-tech fraudsters have developed a new ways of tricking online banking customers, such as Trojan horse and Vishing. (Banking, 2008; Singh, 2007; Anderson, 2007; Howard, 2008 and Randazzo 2004). Phishing attacks is further categorised into two, viz:

2.1.1 Trojan Horse

This is an application in which the program insinuates itself into a user's computer via an email, whereby the program will automatically direct the user of the system to a website which is exactly similar to a Bank website, which built a sophisticated command and-control (C&C) system that completely automates the attacks. Trojan Horse attacks can defeat sophisticated authentication schemes that security experts previously thought rock solid

2.1.2 Vishing

The second well known and fast growing technique is "Vishing" whereby a fraudster will put call directly to the customers and pretends to be a bank representative seeking to verify account information. Fraudsters easily pick up customers vital information such as passwords and account numbers as soon as the customer realise out very important information over the phone.

2.2 Malware

Malware is the term for maliciously crafted software code. Special computer programs now exist that enable intruders to fool customers into believing that traditional security is protecting customers during online banking transactions (Micro 2012 and Singh 2007). Essentially, Malware performs one of the following.

2.2.1 Account Information Theft

Malware capture the keystrokes of login information such as special images or "magic words" whenever a person is trying to log into the Bank website. (Gill, 2011; Anderson 2007 and Iansiti, 2005)

2.2.2 Fake Web Site Substitution

Malware generate web pages that appear to be legitimate but are not. They replace bank's legitimate web site with a page that can look identical, except that the web address will vary in some way. Such a "man in the middle attack" site enables an attacker to intercept customer user information. The attacker adds additional fields to the copy of the web page opened in a customer's browser. When customers submit their information, it is sent to both the bank and the malicious attacker without the knowledge of the customers. (Banking, 2008)

2.2.3 Account Hijacking

Malware hijack the customer's browser and transfer funds without the knowledge of the customers. Ones a customer attempt to login at a bank website, the software launches a hidden browser window on the customer computer, ones a customer successfully logs in to his bank, the software reads the customer's account balance, and creates a secret fund transfer to the intruder-owned accounts. (Voice, 2005)

2.3 PHARMING

Essentially, pharming attacks involve the installation of malicious code into customers' computer; however, pharming can also take place without any conscious action on the customer's part. The common type of pharming attack is when customers open an email, or an email attachment, that installs malicious code on the customer's computer. Later on, the malicious code will delude the customer to log into a fake website that closely resembles a customer bank website. Any information the customers provide during a visit to the fake site is made available to malicious users. (Attacks, 2007; Repository, 2008; Howard, 2008; Singhal, 2008 and Infrastructure, 2007)

3. OBJECTIVES

The major objectives of this paper are: -

- To examine the various online banking frauds in Nigeria commercial banks.
- To provide solutions that will mitigate the frauds in the Nigeria commercial banks.

4. HYPOTHESIS

Find out whether online banking frauds significantly affect electronic banking services by those affected.

H_o: Online banking frauds do not affect electronic banking services.

H_1 : Online banking frauds significantly affect electronic banking services.

5. METHODOLOGY

For the purpose of this study, 5 banks were randomly samples from the 21 banks in Nigeria. These are First Bank, GT Bank, Zenith Bank, UBA and FCMB. Questionnaires were served to 25 customers per sample banks in Kano metropolis. A Likert Scale of 5-points was used to measure the level of agreement or disagreement by the respondents. The response format is as follows:

SA - Strongly Agree
A - Agree
M - Moderate
D - Disagree
SD - Strongly Disagree

Frequency distribution was used to analyze the data collected and examined the pattern of response to

each variable under investigation.

6. DATA ANALYSIS

The analysis of the data is discussed here and since the study seeks to investigate the dimensions of online banking frauds in Nigeria, the frequency counts and percentages were used to capture the responses of the respondents.

Table 1:

Gender Distribution of Respondents			
Banks	*Male*	*Female*	*Total*
FCMB	12	13	25
Zenith	15	10	25
GT Bank	16	9	25
First Bank	17	8	25
UBA	14	11	25
Total	74	51	125

Source: Administered Questionnaire 2012

From **Table 1** above gender distribution of respondents, 60% of the respondents were males, while 40% were women. The highest percentage of males over the females was as a result of the fact that, the male takes more house responsibility than their female counterpart in Nigeria and by extension this may result to the high patronage of online banking than women. Secondly, is because of the eagerness of the men to express their dissatisfaction on the online banking frauds than the women. This was clearly as many of the women are too sceptical to collect the questionnaire immediately they saw the heading online banking scam questionnaire. The frequency counts of males and females differ from one bank to another based on the day of the week the customers were served the questionnaires. The above assertion confirmed the research findings of Amin (2011), Adeoti (2011), Ankit (2011, Musiime (2010), Olatokun (2009), Lloyd (2011), Osabuohien (2008), Metropolis (2010), Al-sukkar (2005) and Ramayah (2003).

Table 2:

Respondents' Age Range		
Age Classification	*Frequency*	*(n) Percentage (%)*
18 – 25 years	17	14
26 – 35 years	49	39
36 – 45 years	34	27
46 – 55 years	16	13
56 and above	9	7
Total	125	100

Source: Administered Questionnaire 2012

From **Table 2** respondents' age classification, 39% of the respondents were within the age bracket of 26-35 years while 27% of the respondents were within the age bracket of 36-45 years. In other words 66% of the respondents were youths whose ages range between 26 and 45 years. The result also tallies with the findings of (Osama, 2008 and Dutta, 2010) and this clearly indicated the level of literacy of the respondents.

Table 3: Respondents' Marital Status

Respondents' Marital Status		
Marital Status	*Frequency (n)*	*Percentage (%)*
Single	37	30
Married	73	59
Divorce	5	4
Widowed	9	7
Total	125	100

Source: Administered Questionnaire 2012

With reference to the **Table 3**, 59% of the respondents were married, 30% were single and 4% and 7% were divorcee and widows / widowers respectively. Students, civil servants and self employed businessmen and women fall into the categories of the singles and the married which constitutes about 86%.

Table 4:

Respondents' Educational Level		
Level of Education	*Frequency (n)*	*Percentage (%) of Customers*
Uneducated	3	2
Primary Education	17	14
Secondary Education	33	26
Tertiary	72	58
Total	125	100

Source: Administered Questionnaire 2012

Table 4 displays the level of education of the customer in all the 5 sampled banks as follows: 58% of the sampled customers have tertiary education, 26% have secondary education while 14% had primary education. 3% of the sampled customers were uneducated.

Table 5:

Distribution of Respondents on Dimensions of Online Banking Frauds		
Dimensions	*Frequency (n)*	*Percentage (%)*
Phishing Attacks	44	35
Vishing	7	6
Account Information Theft	9	7
Fake Web Site Substitution	31	25
Account Hijacking	13	10
Pharming	21	17
Total	125	100

Source: Administered Questionnaire 2012

Table 5, Present the dimensions of online banking frauds in Nigerian commercial banks and the prominent dimensions are ranked in **Table 6**. The dimensions that are 25% and above are Phishing attacks and fake web site substitution. The two constitute about 60% of online banking fraud cases in Nigeria commercial banks.

Table 6 :

Ranking of Dimensions by Respondents		
Dimensions	*Percentage*	*Ranking*
Phishing Attacks	35	1
Fake Web Site Substitution	25	2
Pharming	17	3
Account Hijacking	10	4
Account Information Theft	7	5
Vishing	6	6

Source: Administered Questionnaire 2012

Table 7 :

Distribution of Respondents on Methods of Checkmating Online Banking Frauds		
Methods	*Frequency*	*Percentage*
Use of Pop-up and Email Blocker	33	26
Strong Authentication	47	38
Out of Band Transaction Authentication	15	12
Network Defence in Depth	11	9
Anomalous/Fraudulent Transaction Detection	19	15
Total	125	100

Source: Administered Questionnaire 2012

From the **Table 7** above, 47 respondents (38%) favoured strong Authentication as a method of guarding against online banking frauds, 33 respondents (26%) supported the use of pop-up and an email blocker while 19 respondents amounting to 15% supported the use of Anomalous/Fraudulent Transaction Detection. 12% of the respondents believed that Out of Band Transaction Authentication is very critical to checkmating online banking frauds. Moreover, the remaining 9% supported the use of network defence in depth as a means of protecting online banking frauds.

Table 8 :

Distribution of Respondents on whether Online Banking Frauds Affect Online Banking Services						
Options	*SD*	D	*M*	*A*	*SA*	*Total*
Yes	1	3	5	34	45	88
No	2	15	4	11	5	37
Total	3	18	9	45	50	125

Source: Administered Questionnaire 2012

Table 8 is the observed values of the respondents of bank customers on online banking frauds. To obtain the expected value, we simply use the formula fe = Row Total X Column Total/Grand Total **Table 9** compares the observed frequency of the respondents and expected frequency of online banking frauds' effect on Electronic Banking services.

The χ^2 calculated is 38.35. Hence, by comparing this with χ^2 tabulated at 5% significance level and at (r-1) (c-1) degree of freedom i.e. (2-1) (5-1) = 4 degrees of freedom. Hence, at the 5% level of significance and at 4 degrees of freedom, Chi-square (χ^2) tabulated is 14.9 which is lesser than 2

calculated which is 38.35. Hence, we accept the alternative hypothesis that online banking frauds affect Electronic banking services.

From the foregoing study, it may be evaluated that the higher percentage of male respondents to female suggests that, the men are opposed to the practices of online banking fraud of all kinds. Phishing attacks appear to be the dominant dimension of online banking frauds in Nigeria followed by Fake web site substitution and pharming. While, Vishing fraud is not a common phenomenon in Nigeria, it ranked lowest in the ranking of the dimensions. Strong Authentication rated higher under the method of checkmating or preventing online banking. Online banking frauds tend to erode the customers confidence in the banks, thereby affecting their confidence in utilising electronic banking services.

Table 9:

Frequency of Online Banking Frauds on the Electronic Banking Services				
fo	*Fe*	*fo-fe*	$(fo-fe)^2$	$(fo-fe)^2/fe$
45	35.2	9.8	96.04	2.73
34	31.7	2.3	5.29	0.17
5	6.3	-1.3	1.69	0.27
3	12.7	-9.7	94.09	7.41
1	2.1	-1.1	1.21	0.58
5	14.8	-9.8	96.04	6.49
11	13.32	-3.8	14.44	1.08
4	2.7	1.2	1.44	0.53
15	5.3	9.7	94.09	17.75
2	0.9	11	121	134

χ^2

=38.35

Source: Administered Questionnaire 2012

8. CONCLUSION

As online Banking fraud continues to grow, this put more challenges to the Banking industry. As such, both the Banks and the customers need to proactively mitigate online banking frauds with stronger forms of checkmating online banking frauds that are easy to use and less costly to purchase. Without addressing these considerations, any mutual solution risks not being effective at protecting online Banking frauds can't restore customer confidence in Electronic banking services.

Thus, this paper is of the opinion that every nation has a peculiar online banking fraud that is common to it. The Electronic banking services have great possibilities but that would be dependent on the extent to which the online banking frauds are controlled. There are many other products that are online banking related that have been developed in developed countries. For such products to have a hold in Nigeria, online banking fraud related problems must be solved. Such as ATM frauds, Mobile Banking frauds and electronic fund transfer frauds on point of sale terminals.

9. RECOMMENDATIONS

Like we have rightly observed in the abstract, all the stakeholders have a role to play in minimizing the online banking frauds in Nigeria.

9.1. Solution for Customers

- Customers should stop login to their bank website through a link in an email, even if the email appears to be genuine from their bank. Otherwise, they should key in the web address themselves.
- The customer should always need to be cautious in the encryption process, which appears on the Bank web browser as a locked padlock or unbroken key symbol.
- A secure Banks internet address always beginning with '**https**'
- Customers should be wary of any unexpected or suspicious looking pop-ups that appear during an online banking session.
- A customer should never give out any form of online banking details to anyone either by email or via the phone; Banks don't request such vital information in such ways.

9.2 Solution for Banks

- Banks need to provide and install security software package on customer's computer for free.
- Banks need to employ customized software that records relevant information on online banking transaction so that banks can establish whether an unauthorized transaction has taken place or not.
- Banks need to alert their customers on any suspicious or unusual transaction on their accounts.
- Also, there is the need for Banks to encrypt SMS alert on every transaction on the customer's account.

10. REFERENCE

Adeloye L. A. (2008). E-Banking as New Frontiers for Banks. *Sunday Punch*, September 14, P. 25.

Adeoti, J. O. (2011). Automated Teller Machine (ATM) Frauds in Nigeria : The Way Out, *27*(1), 53–58.

Agbolade, O. K. (2011). Information and Communication Technology And Banks, *1*(4), 102–107.

Akinlolu, A., Lecturer, S., & Oyesola, R. (2008). Journal of Internet Banking and Commerce, *13*(1), 1–15.

Alexander, M. (2004a). Keeping Online Banking Safe : Why Banks Need Geolocation and Other New Techniques Right Now.

Alexander, M. (2004b). Keeping Online Banking Safe : Why Banks Need Geolocation and Other New Techniques Right Now.

Aliyu, A.A. & Tasmin, R (2012). An Exploratory Study on Adoption of Electronic Banking : Underlying Consumer Behaviour and Critical Success Factors . Case of Nigeria ., *2*(1), 1–6.

Aliyu, A. A., & Tasmin, R (2012). The Impact of Information and Communication Technology on Banks: Performance and Customer Service Delivery in the Banking Industry, (1), 80–90.

Anyasi, F. I., & Otubu, P. A. (2009). Mobile Phone Technology in Banking System : Its Economic Effect, *1*(1), 1–5.

Attacks, P. (2007). Journal of Internet Banking and Commerce, *12*(2).

Auta, E. M. (n.d.). Applications of Quantitative Methods to e-Commerce E-Banking in Developing Economy : Empirical Evidence from Nigeria Applications of Quantitative Methods to e-Commerce, 212–222.

Bankole, F. O., & Brown, I. (2011). M. B. A. N, 1–23.

Dutta, S., & Mia, I. (2010). *Technology Report, 2009 – 2010 ICT for Sustainability*.

Howard, R., Thomas, R., Burstein, J., & Bradescu, R. (2008). Cyber Fraud Trends and Mitigation, 9–24.

John, A., & Kaka, E. U. (2011). Information and Communication Technology (ICT) and Banking Industry, *2nd* September, 71–74.

Metropolis, M. (2010). Journal of Internet Banking and Commerce, *15*(2).

Musa, R., & Hassan, F. (2000). Corporate Customers' Adoption of Internet Banking : Case of Klang Valley Business Firm in Malaysia, (June 2000), 13–21.

Needs, I., Banking, O. F., Unique, A. R. E., Intelligence, B., Banking, I. N., Intelligence, O. B. and Business, O., et al. (2007). Operational Business Intelligence in Banking, (1).

Olatokun, W. M., & Science, I. (2009). The Adoption of Automatic Teller Machines in Nigeria : An Application of the Theory of Diffusion of Innovation Louisa Joyce Igbinedion, *6*.

Penang, B., & Kheng, L. L. (2010a). The Impact of Service Quality on Customer Loyalty : A Study of, *2*(2), 57–66.

Penang, B., & Kheng, L. L. (2010b). The Impact of Service Quality on Customer Loyalty : A Study of, *2*(2), 57–66.

Safeena, R., Date, H., & Kammani, A. (2011). Internet Banking Adoption in an Emerging Economy : Indian Consumer ' s Perspective, *2*(1), 56–64.

Safeena, R., Lake, V., & Date, H. (2010). Customer Perspectives on E-business Value: Case Study on Internet Banking. *Journal of Internet Banking and Commerce*, *15*(1), 1–13. Retrieved from http://www.csulb.edu/web/journals/jecr/issues/20044/Paper5.pdf

Sangeetha, J., & Mahalingam, S. (2011). Service quality models in banking: a review. *International Journal of Islamic and Middle Eastern Finance and Management*, *4*(1), 83–103. doi:10.1108/17538391111122221

Shittu, O., Submitted, P., The, T. O., Of, F., Akintola, L., State, O. Y. O., Fulfilment, I. N. P., et al. (2010). The Impact of Electronic Banking in Nigeria Banking System (Critical Appraisal Of Unity Bank Plc), 1–62.

Singh, N. P., Road, M., Warehouse, D., Mining, D., & Projects, E. (2007). Journal of Internet Banking and Commerce, *12*(2).

Singhal, D., & Padhmanabhan, V. (2008). A Study on Customer Perception Towards Internet Banking : Identifying Major Contributing Factors, *5*(1), pp. 101–111.

Voice, C., & President, V. (2005). Authentication : Matching Security, (December).